

GENERATOR MATRIX FOR TWO-DIMENSIONAL CYCLIC CODES OF ARBITRARY LENGTH

ZAHRA SEPASDAR

*Department of Pure Mathematics, Ferdowsi University of Mashhad,
P.O.Box 1159-91775, Mashhad, Iran*

ABSTRACT. Two-dimensional cyclic codes of length $n = \ell s$ over the finite field \mathbb{F} are ideals of the polynomial ring $\mathbb{F}[x, y]/\langle x^s - 1, y^\ell - 1 \rangle$. The aim of this paper, is to present a novel method to study the algebraic structure of two-dimensional cyclic codes of any length $n = s\ell$ over the finite field \mathbb{F} . By using this method, we find the generator polynomials for ideals of $\mathbb{F}[x, y]/\langle x^s - 1, y^\ell - 1 \rangle$ corresponding to two dimensional cyclic codes. These polynomials will be applied to obtain the generator matrix for two-dimensional cyclic codes.

1. INTRODUCTION

One of the important generalizations of the cyclic code is two-dimensional cyclic (TDC) code.

Definition 1.1. Suppose that C is a linear code over \mathbb{F} of length $s\ell$ whose codewords are viewed as $s\ell$ arrays. That is every codeword c in C has the following form

$$c = \begin{pmatrix} c_{0,0} & \cdots & c_{0,\ell-1} \\ c_{1,0} & \cdots & c_{1,\ell-1} \\ \vdots & & \vdots \\ c_{s-1,0} & \cdots & c_{s-1,\ell-1} \end{pmatrix}.$$

If C is closed under row shift and column shift of codewords, then we call C a TDC code of size $s\ell$ over \mathbb{F} .

It is well known that TDC codes of length $n = s\ell$ over the finite field \mathbb{F} are ideals of the polynomial ring $\mathbb{F}[x, y]/\langle x^s - 1, y^\ell - 1 \rangle$.

The characterization for TDC codes, for the first time was presented by Ikai et al. in [1]. Since the method was pure, it didn't help decode these codes. After that, Imai introduced basic theories for binary TDC codes ([2]). The structure of some two-dimensional cyclic codes corresponding to the ideals of $\mathbb{F}[x, y]/\langle x^s - 1, y^{2^k} - 1 \rangle$ is characterized by the present author in [3].

The aim of this paper, is to find the generator matrix for TDC codes of arbitrary length $n = s\ell$ over the finite field \mathbb{F} . To achieve this aim, we present a new method

2010 *Mathematics Subject Classification.* 12E20, 94B05, 94B15, 94B60.

Key words and phrases. two dimensional cyclic code, generator matrix, generator polynomial.
E-mail addresses: zahra.sepasdar@mail.um.ac.ir and zahra.sepasdar@gmail.com.

to characterize ideals of the ring $\mathbb{F}[x, y]/\langle x^s - 1, y^\ell - 1 \rangle$ corresponding to TDC codes, and find generator polynomials for these ideals. Finally, we use these polynomials to obtain the generator matrix for corresponding TDC codes.

Remark 1.2. For simplicity of notation, we write $g(x)$ instead of $g(x) + \langle \mathbf{a} \rangle$ for elements of $\mathbb{F}[x]/\langle \mathbf{a} \rangle$. Similarly, we write $g(x, y)$ instead of $g(x, y) + \langle \mathbf{a}, \mathbf{b} \rangle$ for elements of $\mathbb{F}[x, y]/\langle \mathbf{a}, \mathbf{b} \rangle$.

2. GENERATOR POLYNOMIALS

Set $R := \mathbb{F}[x, y]/\langle x^s - 1, y^\ell - 1 \rangle$ and $S := \mathbb{F}[x]/\langle x^s - 1 \rangle$. Suppose that I is an ideal of R . In this section, we construct ideals I_i of S ($i = 0, \dots, \ell - 1$) and prove that the monic generator polynomials of I_i provide a generating set for I . Since

$$\mathbb{F}[x, y]/\langle x^s - 1, y^\ell - 1 \rangle \cong (\mathbb{F}[x]/\langle x^s - 1 \rangle)[y]/\langle y^\ell - 1 \rangle,$$

an arbitrary element $f(x, y)$ of I can be written uniquely as $f(x, y) = \sum_{i=0}^{\ell-1} f_i(x)y^i$, where $f_i(x) \in S$ for $i = 0, \dots, \ell - 1$. Put

$$I_0 = \{g_0(x) \in S : \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = \sum_{i=0}^{\ell-1} g_i(x)y^i\}.$$

First, we prove that I_0 is an ideal of the ring S . Assume that $g_0(x)$ is an arbitrary element of I_0 . According to the definition of I_0 , there exists $g(x, y) \in I$ such that $g(x, y) = \sum_{i=0}^{\ell-1} g_i(x)y^i$. Now, $xg_0(x) \in I_0$ since I is an ideal of R and $xg(x, y) = \sum_{i=0}^{\ell-1} xg_i(x)y^i$ is an element of I . Besides, I_0 is closed under addition and so I_0 is an ideal of S . It is well-known that S is a principal ideal ring. Therefore, there exists a unique monic polynomial $p_0^0(x)$ in S such that $I_0 = \langle p_0^0(x) \rangle$ and $p_0^0(x)$ is a divisor of $x^s - 1$. So there exists a polynomial $p'_0(x)$ in $\mathbb{F}[x]$ such that $x^s - 1 = p'_0(x)p_0^0(x)$. Now, consider the following equations

$$\begin{aligned} f(x, y) &= f_0(x) + f_1(x)y + \dots + f_{\ell-1}(x)y^{\ell-1} \\ yf(x, y) &= f_0(x)y + f_1(x)y^2 + \dots + f_{\ell-1}(x)y^\ell \\ &= f_{\ell-1}(x) + f_0(x)y + f_1(x)y^2 + \dots + f_{\ell-2}(x)y^{\ell-1}. \quad (y^\ell = 1 \text{ in } R) \end{aligned}$$

Since I is an ideal of R , $yf(x, y) \in I$. So according to the definition of I_0 , $f_{\ell-1}(x) \in I_0$. A similar method can be applied to prove that $f_i(x) \in I_0 = \langle p_0^0(x) \rangle$ for $i = 1, \dots, \ell - 2$. So

$$(1) \quad f_i(x) = p_0^0(x)q_i(x)$$

for some $q_i(x) \in S$. Now, $p_0^0(x) \in I_0$ so according to the definition of I_0 , there exists $\mathbf{p}_0(x, y) \in I$ such that

$$\mathbf{p}_0(x, y) = \sum_{i=0}^{\ell-1} p_i^0(x)y^i.$$

Again since I is an ideal of R , $y^i \mathbf{p}_0(x, y) \in I$ for $i = 1, \dots, \ell - 1$. So according to the definition of I_0 , $p_i^0(x) \in I_0 = \langle p_0^0(x) \rangle$. Therefore,

$$p_i^0(x) = p_0^0(x)t_i^0(x)$$

for some $t_i^0(x) \in S$, and so

$$\mathbf{p}_0(x, y) = p_0^0(x) + \sum_{i=1}^{\ell-1} p_0^0(x) t_i^0(x) y^i.$$

Set

$$\begin{aligned} h_1(x, y) &:= f(x, y) - \mathbf{p}_0(x, y) q_0(x) = \sum_{i=0}^{\ell-1} f_i(x) y^i - q_0(x) \sum_{i=0}^{\ell-1} p_i^0(x) y^i \\ &= f_0(x) + \sum_{i=1}^{\ell-1} f_i(x) y^i - p_0^0(x) q_0(x) - q_0(x) \sum_{i=1}^{\ell-1} p_i^0(x) y^i \\ &= \sum_{i=1}^{\ell-1} f_i(x) y^i - q_0(x) \sum_{i=1}^{\ell-1} p_i^0(x) y^i. \quad (\text{by equation 1}) \end{aligned}$$

Since $f(x, y)$ and $\mathbf{p}_0(x, y)$ are in I and I is an ideal of R , $h_1(x, y)$ is a polynomial in I . Also note that $h_1(x, y)$ is in the form of $h_1(x, y) = \sum_{i=1}^{\ell-1} h_i^1(x) y^i$ for some $h_i^1(x) \in S$. Now, put

$$I_1 = \{g_1(x) \in S : \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = \sum_{i=1}^{\ell-1} g_i(x) y^i\}.$$

By the same method being applied for I_0 , it can be proved that I_1 is an ideal of S . Thus, there exists a unique monic polynomial $p_1^1(x)$ in S such that $I_1 = \langle p_1^1(x) \rangle$ and $p_1^1(x)$ is a divisor of $x^s - 1$. Therefore, there exists a polynomial $p_1'(x)$ in $\mathbb{F}[x]$ such that $x^s - 1 = p_1'(x) p_1^1(x)$. Now, $h_1(x, y) \in I$ so according to the definition of I_1 , $h_1^1(x) \in I_1 = \langle p_1^1(x) \rangle$, and so

$$(2) \quad h_1^1(x) = p_1^1(x) q_1(x)$$

for some $q_1(x) \in S$. And now, $p_1^1(x) \in I_1$ so according to the definition of I_1 , there exists $\mathbf{p}_1(x, y) \in I$ such that

$$\mathbf{p}_1(x, y) = \sum_{i=1}^{\ell-1} p_i^1(x) y^i.$$

Again since I is an ideal of R , $y^i \mathbf{p}_1(x, y) \in I$. So according to the definition of I_0 , $p_i^1(x) \in I_0 = \langle p_0^0(x) \rangle$ for $i = 1, \dots, \ell - 1$. Therefore,

$$p_i^1(x) = p_0^0(x) t_i^1(x)$$

for some $t_i^1(x) \in S$, and so

$$\mathbf{p}_1(x, y) = \sum_{i=1}^{\ell-1} p_0^0(x) t_i^1(x) y^i.$$

Set

$$\begin{aligned}
h_2(x, y) &:= h_1(x, y) - \mathfrak{p}_1(x, y)q_1(x) = \sum_{i=1}^{\ell-1} h_i^1(x)y^i - q_1(x) \sum_{i=1}^{\ell-1} p_i^1(x)y^i \\
&= h_1^1(x)y + \sum_{i=2}^{\ell-1} h_i^1(x)y^i - p_1^1(x)q_1(x)y - q_1(x) \sum_{i=2}^{\ell-1} p_i^1(x)y^i \\
&= \sum_{i=2}^{\ell-1} h_i^1(x)y^i - q_1(x) \sum_{i=2}^{\ell-1} p_i^1(x)y^i. \quad (\text{by equation 2})
\end{aligned}$$

Since $h_1(x, y)$ and $\mathfrak{p}_1(x, y)$ are in I and I is an ideal of R , $h_2(x, y)$ is a polynomial in I in the form of $h_2(x, y) = \sum_{i=2}^{\ell-1} h_i^2(x)y^i$ for some $h_i^2(x) \in S$. Put

$$I_2 = \{g_2(x) \in S : \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = \sum_{i=2}^{\ell-1} g_i(x)y^i\}.$$

Again I_2 is an ideal of S , and so there exists a unique monic polynomial $p_2^2(x)$ in S such that $I_2 = \langle p_2^2(x) \rangle$. Also $p_2^2(x)$ is a divisor of $x^s - 1$, and so there exists a polynomial $p_2'(x)$ in $\mathbb{F}[x]$ such that $x^s - 1 = p_2'(x)p_2^2(x)$. Now, $h_2(x, y) \in I$ so according to the definition of I_2 , $h_2^2(x) \in I_2 = \langle p_2^2(x) \rangle$. So

$$(3) \quad h_2^2(x) = p_2^2(x)q_2(x)$$

for some $q_2(x) \in S$. Besides, $p_2^2(x) \in I_2$ so by definition of I_2 , there exists $\mathfrak{p}_2(x, y) \in I$ such that

$$\mathfrak{p}_2(x, y) = \sum_{i=2}^{\ell-1} p_i^2(x)y^i.$$

Again since I is an ideal of R , $y^i \mathfrak{p}_2(x, y) \in I$. So according to the definition of I_0 , $p_i^2(x) \in I_0 = \langle p_0^0(x) \rangle$. Therefore,

$$p_i^2(x) = p_0^0(x)t_i^2(x)$$

for some $t_i^2(x) \in S$, and so

$$\mathfrak{p}_2(x, y) = \sum_{i=2}^{\ell-1} p_0^0(x)t_i^2(x)y^i.$$

Set

$$\begin{aligned}
h_3(x, y) &:= h_2(x, y) - \mathfrak{p}_2(x, y)q_2(x) = \sum_{i=2}^{\ell-1} h_i^2(x)y^i - q_2(x) \sum_{i=2}^{\ell-1} p_i^2(x)y^i \\
&= h_2^2(x)y^2 + \sum_{i=3}^{\ell-1} h_i^2(x)y^i - p_2^2(x)q_2(x)y^2 - q_2(x) \sum_{i=3}^{\ell-1} p_i^2(x)y^i \\
&= \sum_{i=3}^{\ell-1} h_i^2(x)y^i - q_2(x) \sum_{i=3}^{\ell-1} p_i^2(x)y^i. \quad (\text{by equation 3})
\end{aligned}$$

Therefore, $h_3(x, y)$ is a polynomial in I in the form of $h_3(x, y) = \sum_{i=3}^{\ell-1} h_i^3(x) y^i$ for some $h_i^3(x) \in S$. In the next step, we put

$$I_3 = \{g_3(x) \in S : \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = \sum_{i=3}^{\ell-1} g_i(x) y^i\}.$$

The same procedure is applied to obtain polynomials

$$h_4(x, y), \dots, h_{\ell-2}(x, y), \mathfrak{p}_3(x, y), \dots, \mathfrak{p}_{\ell-2}(x, y)$$

in I and polynomials $q_3(x), \dots, q_{\ell-2}(x)$ in S and construct ideals $I_4, \dots, I_{\ell-2}$. Finally, we set

$$h_{\ell-1}(x, y) := h_{\ell-2}(x, y) - \mathfrak{p}_{\ell-2}(x, y) q_{\ell-2}(x).$$

Thus, $h_{\ell-1}(x, y)$ is a polynomial in I in the form of $h_{\ell-1}(x, y) = h_{\ell-1}^{\ell-1}(x) y^{\ell-1}$. Set

$$I_{\ell-1} = \{g_{\ell-1}(x) \in S : \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = g_{\ell-1}(x) y^{\ell-1}\}.$$

Clearly $I_{\ell-1}$ is an ideal of S . Thus, there exists a unique monic polynomial $p_{\ell-1}^{\ell-1}(x)$ in S such that $I_{\ell-1} = \langle p_{\ell-1}^{\ell-1}(x) \rangle$ and $p_{\ell-1}^{\ell-1}(x)$ is a divisor of $x^s - 1$ (there exists $p'_{\ell-1}(x)$ in $\mathbb{F}[x]$ such that $x^s - 1 = p'_{\ell-1}(x) p_{\ell-1}^{\ell-1}(x)$). Now, $h_{\ell-1}(x, y) \in I$ so according to the definition of $I_{\ell-1}$, $h_{\ell-1}^{\ell-1}(x) \in I_{\ell-1} = \langle p_{\ell-1}^{\ell-1}(x) \rangle$. So

$$(4) \quad h_{\ell-1}^{\ell-1}(x) = q_{\ell-1}(x) p_{\ell-1}^{\ell-1}(x)$$

for some $q_{\ell-1}(x) \in S$. And now, $p_{\ell-1}^{\ell-1}(x) \in I_{\ell-1}$ so according to the definition of $I_{\ell-1}$, there exists $\mathfrak{p}_{\ell-1}(x, y) \in I$ such that $\mathfrak{p}_{\ell-1}(x, y) = p_{\ell-1}^{\ell-1}(x) y^{\ell-1}$. Therefore, by equation 4

$$h_{\ell-1}(x, y) = h_{\ell-1}^{\ell-1}(x) y^{\ell-1} = q_{\ell-1}(x) p_{\ell-1}^{\ell-1}(x) y^{\ell-1} = q_{\ell-1}(x) \mathfrak{p}_{\ell-1}(x, y).$$

Again since I is an ideal of R , $y \mathfrak{p}_{\ell-1}(x, y) \in I$. So according to the definition of I_0 , $p_{\ell-1}^{\ell-1}(x) \in I_0 = \langle p_0^0(x) \rangle$. Thus,

$$p_{\ell-1}^{\ell-1}(x) = p_0^0(x) t_{\ell-1}^{\ell-1}(x)$$

for some $t_{\ell-1}^{\ell-1}(x) \in S$, and so

$$\mathfrak{p}_{\ell-1}(x, y) = p_0^0(x) t_{\ell-1}^{\ell-1}(x) y^{\ell-1}.$$

Therefore, for an arbitrary element $f(x, y) \in I$ we show that

$$\begin{aligned} h_1(x, y) &:= f(x, y) - \mathfrak{p}_0(x, y) q_0(x) \\ h_2(x, y) &:= h_1(x, y) - \mathfrak{p}_1(x, y) q_1(x) \\ h_3(x, y) &:= h_2(x, y) - \mathfrak{p}_2(x, y) q_2(x) \\ &\dots \\ h_{\ell-1}(x, y) &:= h_{\ell-2}(x, y) - \mathfrak{p}_{\ell-2}(x, y) q_{\ell-2}(x) \\ h_{\ell-1}(x, y) &= q_{\ell-1}(x) \mathfrak{p}_{\ell-1}(x, y). \end{aligned}$$

So

$$\begin{aligned} f(x, y) &= \mathfrak{p}_0(x, y) q_0(x) + \mathfrak{p}_1(x, y) q_1(x) + \mathfrak{p}_2(x, y) q_2(x) \\ &\quad + \dots + \mathfrak{p}_{\ell-2}(x, y) q_{\ell-2}(x) + \mathfrak{p}_{\ell-1}(x, y) q_{\ell-1}(x). \end{aligned}$$

Since $\mathbf{p}_i(x, y) \in I$ for $i = 0, \dots, \ell - 1$ and $f(x, y)$ is an arbitrary element of I and I is an ideal of R , we conclude that

$$I = \langle \mathbf{p}_0(x, y), \dots, \mathbf{p}_{\ell-1}(x, y) \rangle,$$

where $\mathbf{p}_j(x, y) = \sum_{i=0}^{\ell-1} p_0^0(x) t_i^j(x) y^i$. So $\{\mathbf{p}_0(x, y), \mathbf{p}_1(x, y), \dots, \mathbf{p}_{\ell-1}(x, y)\}$ is a set of generating polynomials for I .

In the next theorem, we introduce the generator matrix for TDC codes.

Theorem 2.1. *Suppose that I is an ideal of $\mathbb{F}[x, y]/\langle x^s - 1, y^\ell - 1 \rangle$ and is generated by $\{\mathbf{p}_0(x, y), \dots, \mathbf{p}_{\ell-1}(x, y)\}$, which obtained from the above method. Then the set*

$$\begin{aligned} &\{\mathbf{p}_0(x, y), x\mathbf{p}_0(x, y), \dots, x^{s-a_0-1}\mathbf{p}_0(x, y), \\ &\mathbf{p}_1(x, y), x\mathbf{p}_1(x, y), \dots, x^{s-a_1-1}\mathbf{p}_1(x, y), \\ &\vdots \\ &\mathbf{p}_{\ell-1}(x, y), x\mathbf{p}_{\ell-1}(x, y), \dots, x^{s-a_{\ell-1}-1}\mathbf{p}_{\ell-1}(x, y)\} \end{aligned}$$

forms an \mathbb{F} -basis for I , where $a_i = \deg(p_i^0(x))$.

Proof. Assume that $l_0(x), \dots, l_{\ell-1}(x)$ are polynomials in $\mathbb{F}[x]$ such that $\deg(l_i(x)) < s - a_i$ and $l_0(x)\mathbf{p}_0(x, y) + \dots + l_{\ell-1}(x)\mathbf{p}_{\ell-1}(x, y) = 0$. These imply the following equation in S

$$l_0(x)p_0^0(x) = 0.$$

Therefore, $l_0(x)p_0^0(x) = s(x)(x^s - 1)$ for some $s(x) \in \mathbb{F}[x]$. Now, the degree of x in the right side of this equation is at least s but since $\deg(p_0^0(x)) = a_0$ and $\deg(l_0(x)) < s - a_0$, the degree of x in the left side of this equation is at most $s - 1$. So we get $l_0(x) = 0$. Similar arguments yield $l_i(x) = 0$ for $i = 1, \dots, \ell - 1$. \square

3. CONCLUSION

In this paper, we present a novel method for studying the structure of TDC codes of length $n = s\ell$. This leads to studying the structure of ideals of the ring $\mathbb{F}[x, y]/\langle x^s - 1, y^\ell - 1 \rangle$. By using the novel method, we obtain generating sets of polynomials and generator matrix for TDC codes.

REFERENCES

- [1] T. Ikai, H. Kosako, Y. Kojima, *Two-Dimensional Cyclic Codes*, Electronics and Communications in Japan 57-A (1975), pp. 27-35.
- [2] H. Imai, *A Theory of Two-Dimensional Cyclic Codes*, Information and Control **34** (1977), pp. 1-21.
- [3] Z. Sepasdar, K. Khashyarmansh, *Characterizations of some two-dimensional cyclic codes correspond to the ideals of $\mathbb{F}[x, y]/\langle x^s - 1, y^{2^k} - 1 \rangle$* , Finite Fields and Their Applications **41** (2016), pp. 97-112.